On an Inference System for a Hybrid Process Calculus

Zining Cao[1,2]

[1]State Key Laboratory for Civil Aircraft Flight Simulation
Shanghai Aircraft Design and Research Institute
Shanghai 201210, China
[2]Department of Computer Science and Technology
Nanjing University of Aeronautics & Astronautics
Nanjing 210016, China

***Abstract*—In this paper, we propose a hybrid process calculus. This hybrid process calculus can be used to describe hybrid properties and nondeterministic properties of software. The concrete bisimulation and symbolic bisimulation of this hybrid process calculus are proposed. We then prove the equivalence between these two bisimulation. An inference system for the symbolic bisimulation of this hybrid process calculus is given. At last, we prove the soundness and completeness of the inference system.**

***Keywords*—hybrid process calculus; symbolic bisimulation; inference system**

I. INTRODUCTION

Hybrid system is a kind of mixed discrete-continuous system. A paradigmatic example of a mixed discrete-continuous system is a digital controller of an analog plant. The discrete state of the controller is modelled by the vertices of a graph (control modes), and the discrete dynamics of the controller is modelled by the edges of the graph (control switches). The continuous state of the plant is modelled by points in $\mathbf{R}^n$, and the continuous dynamics of the plant is modelled by flow conditions such as differential equations. The behavior of the plant depends on the state of the controller: each control mode determines a flow condition, and each control switch may cause a discrete change in the state of the plant, as determined by a jump condition. Dually, the behavior of the controller depends on the state of the plant: each control mode continuously observes an invariant condition of the plant state, and by violating the invariant condition, a continuous change in the plant state will cause a control switch.

There are several works on models of hybrid systems such as [2], [3], [4], [7], and [12]. But there are seldom works on sound and complete inference systems for bisimulation of hybrid systems. For examples, some sound inference systems for bisimulation were given in [2] and [4], whereas these inference system were not proved complete. In this paper, we aim to propose a sound and complete inference system for bisimulation of hybrid systems. To this end, we firstly present a hybrid process calculus including its syntax, operational semantics and concrete bisimulation in this paper. Then the symbolic labelled transition system and symbolic bisimulation are also presented. We prove the equivalence of concrete bisimulation and symbolic bisimulation. Furthermore, we present an inference system for symbolic bisimulation. Finally, the soundness and completeness of this inference system are studied.

This paper is organized as follows: Section 2 gives a hybrid process calculus including its syntax, operational semantics and concrete bisimulation. In Section 3, we propose a symbolic theory for this hybrid process calculus including symbolic labelled transition system and symbolic bisimulation for hybrid process calculus. Furthermore, we prove the equivalence between concrete bisimulation and symbolic bisimulation. In Section 4, we give a complete inference system for this hybrid process. The soundness and completeness of the inference system are also proved. The paper is concluded in Section 5.

II. HYBRID PROCESS CALCULUS

There are many works about process algebras for hybrid systems, for example, [2], [3], [4], [7], and [12]. A comparative study of these process algebras is referred to [9]. The main aim of this paper is to propose a sound and complete inference for bisimulation of hybrid systems. To this end, we present a simple hybrid process calculus which has a relatively small number of operators and a simpler semantics. Therefore it is easier to give a complete inference system than other process algebras. The syntax, operational semantics and concrete bisimulation of this process calculus are given in this section.

A. Syntax of Hybrid Process Calculus

To give the syntax of hybrid process calculus, we first present the syntax and semantics of predication logical formulas.

Predication logical formulas are defined by the following grammar:

$\Phi, \Psi ::= x \bowtie u(x_1, ..., x_n) \mid \neg\Phi \mid \Phi \wedge \Psi \mid \forall x.\Phi$, where $\bowtie \in \{=, \neq, \geq, >, <, \leq\}$, x is a variable, $u(x_1, ..., x_n)$ is a real function with parameters $x_1, ..., x_n$, i.e., $u(r_1, ..., r_n) = r$ where $r_1, ..., r_n, r \in \mathbf{R}$ and $\mathbf{R}$ is the set of real numbers. We denote the set of variable $\{t, v_1, v_2, ..., v_n, ...\}$ as Var^0, denote the set of variable $\{t', v_1', v_2', ..., v_n', ...\}$ as Var', and denote $Var^0 \cup Var' = Var$. Informally, variables $v_1', ..., v_n'$

represent the new values taken by the variables $v_1, ..., v_n$ after a transition. Variable t represents the time variable.

The satisfiability relation $\models$ is defined between assignment θ and formula Φ as follows, where θ is a function such that the domain of θ is a subset of Var and the range of θ is $\mathbf{R}$, and free variables in Φ is in the domain of θ.

(1) $\theta \models x \bowtie u(x_1, ..., x_n)$ if $\theta(x) \bowtie u(\theta(x_1), ..., \theta(x_n))$;

(2) $\theta \models \neg\Phi$ if $\theta \not\models \Phi$;

(3) $\theta \models \Phi \wedge \Psi$ if $\theta \models \Phi$ and $\theta \models \Psi$;

(4) $\theta \models \forall x.\Phi$ if $\theta \models \Phi\{a/x\}$ for any a, where $\{s/t\}$ means replacing t by s.

We write $\Phi \models \Psi$ to mean that $\theta \models \Phi$ implies $\theta \models \Psi$ for any θ, and write $\models \Psi$ to mean that $\theta \models \Psi$ for any θ.

The formal definition of process is given as follows:

$P ::= 0 \mid X \mid P + P \mid \varepsilon(\Phi_1, \Phi_2).P \mid a(\Psi_1, \Psi_2).P \mid fixX.P$, where Φ_1 is a predication logical formulas with free variables in Var^0; Φ_2 is a predication logical formulas with free variables in Var; ε is an internal action which is invisible for observer; Ψ_1 is a predication logical formulas with free variables in Var^0; Ψ_2 is a predication logical formulas with free variables in Var; a is an external action which is visible for observer; all process variables in $fixX.P$ are guarded by action prefix. The class of processes is denoted as Pr.

Informally, 0 denotes inaction. $P_1 + P_2$ expresses nondeterministic choice of processes P_1 and P_2. $\varepsilon(\Phi_1, \Phi_2).P$ can perform an internal action ε under condition Φ_1, then continues as P, and the change of variables satisfies Φ_2. $a(\Psi_1, \Psi_2).P$ can perform an external action a under condition Ψ_1, then continues as P, and the change of variables satisfies Ψ_2. $fixX.P$ is a recursive definition of process.

B. Labelled Transition System of Hybrid Process Calculus

The operational semantics of hybrid process calculus is given in Table 1. We have omitted the symmetric rule of the nondeterministic operator.

The labelled transition system consists of a collection of relations of the form $\langle P, \rho\rangle \xrightarrow{\varepsilon(\Phi_1,\Phi_2),T} \langle Q, \sigma\rangle$ or $\langle P, \rho\rangle \xrightarrow{a(\Psi_1,\Psi_2)} \langle Q, \sigma\rangle$, where P, Q are processes, and ρ, σ are configurations. A configuration is a function ρ such that $\rho(x) \in \mathbf{R}$ for any $x \in Var^0$. A configuration represents an possible assignment of variables. The class of configurations is denoted as C. The transition $\langle P, \rho\rangle \xrightarrow{\varepsilon(\Phi_1,\Phi_2),T} \langle Q, \sigma\rangle$ means that the process P at configuration ρ can realize the action $\varepsilon(\Phi_1, \Phi_2)$, and becomes Q at configuration σ after T units of time. The transition $\langle P, \rho\rangle \xrightarrow{a(\Psi_1,\Psi_2)} \langle Q, \sigma\rangle$ means that the process P at configuration ρ can realize the action $a(\Psi_1, \Psi_2)$, and becomes Q at configuration σ. We denote by $\rho[x \leftarrow U]$ a new configuration that is the same as ρ except that $\rho[x \leftarrow U](x) = U$, and denote by $\rho[x \Leftarrow x']$ a function such that $f(x') = \rho(x)$ for any x in the domain of ρ. In the following, for function $\rho : X \to \mathbf{R}$ and function $\sigma : Y \to \mathbf{R}$ with condition $X \cap Y = \emptyset$, we use $\rho \cup \sigma$ to denote function f such that $f(x) = \rho(x)$ when $x \in X$ and $f(x) = \sigma(x)$ when $x \in Y$.

$$TAU : \langle \varepsilon(\Phi_1, \Phi_2).P, \rho\rangle \xrightarrow{\varepsilon(\Phi_1,\Phi_2),T} \langle P, \rho'\rangle, \text{ where } T \in \mathbf{R}, \forall \delta \in [0, T].\rho[t \leftarrow \rho(t) + \delta] \models \Phi_1,\ \rho'(t) = \rho(t) + T, \rho \cup (\rho'[x \Leftarrow x']) \models \Phi_2.$$

$$ACT : \langle a(\Psi_1, \Psi_2).P, \rho\rangle \xrightarrow{a(\Psi_1,\Psi_2)} \langle P, \rho'\rangle, \text{ where } \rho \models \Psi_1, \rho \cup (\rho'[x \Leftarrow x']) \models \Psi_2.$$

$$SUM : \frac{\langle P_1, \rho\rangle \xrightarrow{\alpha} \langle P_1', \rho'\rangle}{\langle P_1 + P_2, \rho\rangle \xrightarrow{\alpha} \langle P_1', \rho'\rangle}$$

$$REC : \frac{\langle P\{fixX.P/X\}, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}{\langle fixX.P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}$$

Table 1: Operational semantics of hybrid process calculus

An example: Let process $P = \varepsilon(\Phi_1, \Phi_2).a(\Psi_1, \Psi_2).0 = \varepsilon(x_1 + x_2 + t \le 2y + 1,\ x_1' = tx_1 \wedge x_2' = 2x_2 \wedge y' \le 2x_2' - x_1).a(x_1 + x_2 \ge y,\ x_1' = 2x_1 \wedge x_2' = x_2).0$. Then at configuration ρ such that $\rho(t) = 0$, $\rho(x_1) = 1$, $\rho(x_2) = 2$, $\rho(y) = 3$,we have $\langle P, \rho\rangle \xrightarrow{\varepsilon(\Phi_1,\Phi_2),2} \langle P', \rho'\rangle$, where $P' = a(\Psi_1, \Psi_2).0 = a(x_1 + x_2 \ge y, x_1' = 2x_1 \wedge x_2' = x_2).0$, ρ' is a configuration such that $\rho'(t) = 2$, $\rho'(x_1) = 2$, $\rho'(x_2) = 4$, $\rho'(y) \le 6$. Furthermore, $\langle P', \rho'\rangle \xrightarrow{a(\Psi_1,\Psi_2)} \langle 0, \rho''\rangle$, where ρ'' is a configuration such that $\rho''(t) = 2$, $\rho''(x_1) = 4$, $\rho''(x_2) = 4$, $\rho''(y) \in \mathbf{R}$.

C. Concrete Bisimulation

Now we propose a concrete bisimulation for hybrid process calculus. Intuitively, P and Q are concrete bisimilar if whenever P can perform an action under the configuration ρ, Q can also perform the same action under the configuration ρ.

Definition 2. A symmetric relation $R \in (Pr \times C) \times (Pr \times C)$ is called a concrete bisimulation if whenever $\langle P, \rho\rangle\ R\ \langle Q, \rho\rangle$,

(1) $\langle P, \rho\rangle \xrightarrow{\varepsilon(\Phi_1^P,\Phi_2^P),T} \langle P', \rho'\rangle$ implies that there exists Q' such that $\langle Q, \rho\rangle \xrightarrow{\varepsilon(\Phi_1^Q,\Phi_2^Q),T} \langle Q', \rho'\rangle$ and $\langle P', \rho'\rangle\ R\ \langle Q', \rho'\rangle$;

(2) $\langle P, \rho\rangle \xrightarrow{a(\Psi_1^P,\Psi_2^P)} \langle P', \rho'\rangle$ with $a \neq \varepsilon$ implies that there exists Q' such that $\langle Q, \rho\rangle \xrightarrow{a(\Psi_1^Q,\Psi_2^Q)} \langle Q', \rho'\rangle$ and $\langle P', \rho'\rangle\ R\ \langle Q', \rho'\rangle$.

We write $\langle P, \rho\rangle \sim \langle Q, \rho\rangle$ if there is a concrete bisimulation R such that $\langle P, \rho\rangle\ R\ \langle Q, \rho\rangle$.

We write $P \sim_C Q$ if $\langle P, \rho\rangle \sim \langle Q, \rho\rangle$ for any ρ.

Remark: In the above definition, we do not require that Φ_1^P and Φ_1^Q (Φ_2^P and Φ_2^Q, or Ψ_1^P and Ψ_1^Q, or Ψ_2^P and Ψ_2^Q) are logical equivalent since by the operational semantics of hybrid process calculus, $\langle P, \rho\rangle \xrightarrow{\varepsilon(\Phi_1^P,\Phi_2^P),T} \langle P', \rho'\rangle$ is permitted if $\forall \delta \in [0, T].\rho[t \leftarrow \rho(t) + \delta] \models \Phi_1^P$, and $\langle Q, \rho\rangle \xrightarrow{\varepsilon(\Phi_1^Q,\Phi_2^Q),T} \langle Q', \rho'\rangle$ is permitted if $\forall \delta \in [0, T].\rho[t \leftarrow \rho(t) + \delta] \models \Phi_1^Q$, which means $\forall \delta \in [0, T].\rho[t \leftarrow \rho(t) + \delta] \models \Phi_1^P \leftrightarrow \Phi_1^Q$. Therefore the logical equivalent relation between Φ_1^P and Φ_1^Q is implied by the side condition of operational semantics of hybrid process calculus. The cases of Φ_2^P and Φ_2^Q, Ψ_1^P and Ψ_1^Q, Ψ_2^P and Ψ_2^Q are similar.

 ISBN: 978-1-61208-277-6

III. A SYMBOLIC THEORY FOR HYBRID PROCESS CALCULUS

In this section, a symbolic labelled transition system and a symbolic bisimulation equivalence are presented. The full abstraction property, i.e., the equivalence between this symbolic bisimulation and the concrete bisimulation, is shown. The symbolic semantics is necessary for an efficient implementation of the calculus in automated tools exploring state spaces, and the full abstraction property means processes are bisimilar in the symbolic setting if they are bisimilar in the original semantics.

A. Symbolic Labelled Transition System

The symbolic operational semantics of hybrid process calculus is given in Table 2. We have omitted the symmetric of the nondeterministic. The labelled transition system consists of a collection of relations of the form $P \xrightarrow{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'} Q$ or $P \xrightarrow{\Gamma,a(\Psi_1,\Psi_2),\Gamma'} Q$. The transition $P \xrightarrow{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'} Q$ means that the process P can realize the action $\varepsilon(\Phi_1,\Phi_2)$ if condition Γ is true, and becomes Q where Γ' is true after T units of time. The transition $P \xrightarrow{\Gamma,a(\Psi_1,\Psi_2),\Gamma'} Q$ means that the process P can realize the action $a(\Psi_1,\Psi_2)$ if condition Γ is true, and becomes Q where Γ' is true.

In the following, we use $(\exists \vec{X} .\Phi)\{\vec{X} / \vec{X'}\}$ to abbreviate $(\exists x_1...\exists x_m.\Phi)\{x_1,...,x_m/x'_1,...,x'_m\}$, where the set of free variables in Φ is $\{x_1,...,x_m,x'_1,...,x'_m\}$.

$$TAU : \varepsilon(\Phi_1,\Phi_2).P \xrightarrow{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'} P, \text{ where } T \in \mathbf{R},$$
$$\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_1\{t+\delta/t\},$$
$$\models (\exists \vec{X} .(\Gamma \wedge \Phi_2 \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'.$$

$$ACT : a(\Psi_1,\Psi_2).P \xrightarrow{\Gamma,a(\Psi_1,\Psi_2),\Gamma'} P, \text{ where } \models \Gamma \rightarrow \Psi_1,$$
$$\models (\exists \vec{X} .(\Gamma \wedge \Psi_2))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'.$$

$$SUM : \frac{P_1 \xrightarrow{\Gamma,\alpha,\Gamma'} P'_1}{P_1 + P_2 \xrightarrow{\Gamma,\alpha,\Gamma'} P'_1}$$

$$REC : \frac{P\{fixX.P/X\} \xrightarrow{\Gamma,\alpha,\Gamma'} P'}{fixX.P \xrightarrow{\Gamma,\alpha,\Gamma'} P'}$$

Table 2: Symbolic operational semantics of hybrid process calculus

An example: Let process $P = \varepsilon(\Phi_1,\Phi_2).Q = \varepsilon(x_1+x_2 \leq 2y+1,\ y' \leq 2x'_2 - x_1).Q$, formula $\Gamma = (t = 0 \wedge x_1 \geq 0 \wedge x_1 + x_2 \leq 3 \wedge y = 3)$. Then we have $P \xrightarrow{\Gamma,(\varepsilon(\Phi_1,\Phi_2),2),\Gamma'} Q$, where $\Gamma' = (t \geq 2 \wedge y \leq 2x_2)$.

B. Symbolic Bisimulation

In this section we define a symbolic version of concrete bisimulation for hybrid process calculus. Symbolic bisimulation is defined as a family of binary relations indexed by a predication logical formula which expresses variable constraints.

Definition 3. A collection of formulas Σ is a partition of Φ if for any θ it holds that $\theta \models \Phi$ implies $\theta \models \Psi$ for some $\Psi \in \Sigma$. A finite partition of Φ is a finite collection of formulas which is a partition of Φ.

Definition 4. A symmetric relation $R \in Pr \times Pr$ with respect to the formula Γ is called a symbolic bisimulation if whenever $P\ R^{\Gamma}\ Q$,

(1) $P \xrightarrow{\Gamma,(\varepsilon(\Phi_1^P,\Phi_2^P),T),\Gamma'_P} P'$ implies that there exists a finite partition $\Sigma = \{\phi_i \mid i \in I\}$, $\models \Gamma \wedge \Phi_1^P \leftrightarrow \vee_{i\in I}\phi_i$, for any ϕ_i there exists a finite partition $\Pi = \{\chi_j \mid j \in J\}$ such that $\models \phi_i \wedge \Phi_2^P \leftrightarrow \vee_{j\in J}\chi_j$, for any χ_j there exists Q' such that $Q \xrightarrow{\Gamma,(\varepsilon(\Phi_1^Q,\Phi_2^Q),T),\Gamma'_Q} Q'$ and $\phi_i \models \Gamma \wedge \Phi_1^Q$, $\chi_j \models \Gamma \wedge \Phi_2^Q$ and $P'\ R^{(\exists \vec{X}.\chi_j \wedge t' = t+T)\{\vec{X}/\vec{X'}\}}\ Q'$;

(2) $P \xrightarrow{\Gamma,a(\Psi_1^P,\Psi_2^P),\Gamma'_P} P'$ with $a \neq \varepsilon$ implies that there exists a finite partition $\Sigma = \{\phi_i \mid i \in I\}$, $\models \Gamma \wedge \Psi_1^P \leftrightarrow \vee_{i\in I}\phi_i$, for any ϕ_i there exists a finite partition $\Pi = \{\chi_j \mid j \in J\}$ such that $\models \phi_i \wedge \Psi_2^P \leftrightarrow \vee_{j\in J}\chi_j$, for any χ_j there exists Q' such that $Q \xrightarrow{\Gamma,.a(\Psi_1^Q,\Psi_2^Q),\Gamma'_Q} Q'$ and $\phi_i \models \Gamma \wedge \Psi_1^Q$, $\chi_j \models \Gamma \wedge \Psi_2^Q$ and $P'\ R^{(\exists \vec{X}.\chi_j)\{\vec{X}/\vec{X'}\}}\ Q'$.

We write $P \sim_S^{\Gamma} Q$ if there is a symbolic bisimulation R such that $P\ R^{\Gamma}\ Q$.

C. Equivalence Between Concrete Bisimulation and Symbolic Bisimulation

In this section, we will prove the equivalence between concrete bisimulation and symbolic bisimulation. Thus to give a complete inference system for concrete bisimulation, it is enough to give a complete inference system for symbolic bisimulation.

To prove Proposition 1 which states the equivalence between concrete bisimulation and symbolic bisimulation, we need some lemmas.

Lemma 1. There exists ρ such that $\rho \cup \rho' \models \Gamma \Leftrightarrow \rho' \models (\exists x_1...\exists x_m.\Gamma)$, where the domain of ρ is $\{x_1,...,x_m\}$, the domain of ρ' is $\{y_1,...,y_n\}$, $\{x_1,...,x_m\} \cap \{y_1,...,y_n\} = \emptyset$.

Proof. See Appendix A. ■

The following lemma gives the corresponding relation between symbolic transition and concrete transition.

Lemma 2. (1) Given Γ and Γ', if for any $\rho \models \Gamma$, there is ρ', such that $\rho' \models \Gamma'$, $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Phi_2$, and $\langle P,\rho\rangle \xrightarrow{\varepsilon(\Phi_1,\Phi_2),T} \langle P',\rho'\rangle$, then $P \xrightarrow{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'} P'$, where $\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_1\{t+\delta/t\}$, $\models (\exists \vec{X} .(\Gamma \wedge \Phi_2 \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$;

(2) Given Γ and Γ', if for any $\rho \models \Gamma$, there is ρ', such that $\rho' \models \Gamma'$, $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Psi_2$, and $\langle P,\rho\rangle \xrightarrow{a(\Psi_1,\Psi_2)} \langle P',\rho'\rangle$, then $P \xrightarrow{\Gamma,a(\Psi_1,\Psi_2),\Gamma'} P'$, where $\models \Gamma \rightarrow \Psi_1$, $\models (\exists \vec{X} .(\Gamma \wedge \Psi_2))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$;

(3) $P \xrightarrow{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'} P'$ implies for any $\rho \models \Gamma$, there is ρ', such that $\rho' \models \Gamma'$ and $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Phi_2$, $\langle P,\rho\rangle \xrightarrow{\varepsilon(\Phi_1,\Phi_2),T} \langle P',\rho'\rangle$, where $\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_1\{t+\delta/t\}$, $\models (\exists \vec{X} .(\Gamma \wedge \Phi_2 \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$;

(4) $P \xrightarrow{\Gamma, a(\Psi_1,\Psi_2), \Gamma'} P'$ implies for any $\rho \models \Gamma$, there is ρ', such that $\rho' \models \Gamma'$ and $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Psi_2$, $\langle P, \rho\rangle \xrightarrow{a(\Psi_1,\Psi_2)} \langle P', \rho'\rangle$, where $\models \Gamma \rightarrow \Psi_1$, $\models (\exists \vec{X} .(\Gamma \wedge \Psi_2))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$.

Proof. See Appendix B. ■

The following lemma shows the image-finite property of symbolic transition.

Lemma 3. (1) For any P and Γ, there are finitely many $\varepsilon(\Phi_1^P, \Phi_2^P)$, such that $P \xrightarrow{\Gamma, (\varepsilon(\Phi_1^P,\Phi_2^P), T), \Gamma'_P} P'$;

(2) For any P and Γ, there are finitely many $a(\Psi_1^P, \Psi_2^P)$, such that $P \xrightarrow{\Gamma, a(\Psi_1^P,\Psi_2^P), \Gamma'_P} P'$.

Proof. By induction on the inference length of $P \xrightarrow{\Gamma, (\varepsilon(\Phi_1^P,\Phi_2^P), T), \Gamma'_P} P'$ or $P \xrightarrow{\Gamma, a(\Psi_1^P,\Psi_2^P), \Gamma'_P} P'$. ■

In the following, we show that any process is symbolic bisimilar to a "normal process".

Lemma 4. For any P and Γ, there exists a process in the form of $\Sigma_{l\in L}\varepsilon(\Phi_{l1}, \Phi_{l2}).P_l + \Sigma_{m\in M} a_m(\Psi_{m1}, \Psi_{m2}).P_m$ such that $P \sim_S^\Gamma \Sigma_{l\in L}\varepsilon(\Phi_{l1}, \Phi_{l2}).P_l + \Sigma_{m\in M} a_m(\Psi_{m1}, \Psi_{m2}).P_m$.

Proof. By Lemma 3 and by induction on the structure of P. ■

The equivalence between concrete bisimulation and symbolic bisimulation is given in the following proposition.

Proposition 1. For any $\rho \models \Gamma$, $\langle P, \rho\rangle \sim \langle Q, \rho\rangle \Leftrightarrow P \sim_S^\Gamma Q$.

Proof. See Appendix C. ■

Remark: For the symbolic bisimulation, for a transition from P, there should be a finite partition from Q. In the proof of Proposition 1, we show the existence of such finite partition.

IV. A Complete Inference System for Hybrid Process Calculus

In this section, we give an inference system for symbolic bisimulation. The soundness and completeness of this inference system are also studied.

A. An Inference System for Bisimulation of Hybrid Process Calculus

An inference system for symbolic bisimulation consists of the following rules. The rules are in the form of $\frac{A_1,\ ...,\ A_n}{B}$, which means B is true if $A_1,\ ...,\ A_n$ are all true. In these rules, the notation $\Gamma \triangleright P = Q$ means process P is equivalent to process Q if formula Γ is true.

(1) $$\frac{\begin{array}{c}\Gamma \models \Phi_1 \leftrightarrow \Phi_3,\\ \models \exists t.(t' \geq t \wedge \Phi_1 \wedge \Gamma \wedge \Phi_2) \leftrightarrow \exists t.(t' \geq t \wedge \Phi_3 \wedge \\ \Gamma \wedge \Phi_4)\end{array}}{\Gamma \triangleright \varepsilon(\Phi_1, \Phi_2).P = \varepsilon(\Phi_3, \Phi_4).P}$$

(2) $$\frac{\begin{array}{c}\Gamma \models \Phi_1,\\ (\exists \vec{X} .(\Phi_1 \wedge \Gamma \wedge \Phi_2 \wedge t' \geq t)\{\vec{X} / \vec{X'}\} \triangleright P = Q\end{array}}{\Gamma \triangleright \varepsilon(\Phi_1, \Phi_2).P = \varepsilon(\Phi_1, \Phi_2).Q}$$

(3) $$\frac{\Gamma \models \Psi_1 \leftrightarrow \Psi_3,\ \models (\Psi_1 \wedge \Gamma \wedge \Psi_2) \leftrightarrow (\Psi_3 \wedge \Gamma \wedge \Psi_4)}{\Gamma \triangleright a(\Psi_1, \Psi_2).P = a(\Psi_3, \Psi_4).P}$$

(4) $$\frac{\Gamma \models \Psi_1,\ (\exists \vec{X} .(\Psi_1 \wedge \Gamma \wedge \Psi_2))\{\vec{X} / \vec{X'}\} \triangleright P = Q}{\Gamma \triangleright a(\Psi_1, \Psi_2).P = a(\Psi_1, \Psi_2).Q}$$

(5) $$\frac{\Gamma \models \neg\Phi_1}{\Gamma \triangleright \varepsilon(\Phi_1, \Phi_2).P = 0}$$

(6) $$\frac{\Gamma \models \neg\Psi_1}{\Gamma \triangleright a(\Psi_1, \Psi_2).P = 0}$$

(7) $$\frac{\Gamma \models \neg\Phi_2}{\Gamma \triangleright \varepsilon(\Phi_1, \Phi_2).P = 0}$$

(8) $$\frac{\Gamma \models \neg\Psi_2}{\Gamma \triangleright a(\Psi_1, \Psi_2).P = 0}$$

(9) $$\frac{\Gamma \triangleright P = Q}{\Gamma \triangleright P + R = Q + R}$$

(10) $$\frac{}{\Gamma \triangleright fixX.P = P\{fixX.P/X\}}$$

(11) $$\frac{\Gamma \triangleright P = Q\{P/X\}}{\Gamma \triangleright P = fixX.Q}$$

(12) $$\frac{\Gamma \triangleright P = Q}{\Gamma \triangleright fixX.P = fixX.Q}$$

(13) $$\frac{}{\Gamma \triangleright P = P}$$

(14) $$\frac{\Gamma \triangleright P = Q}{\Gamma \triangleright Q = P}$$

(15) $$\frac{\Gamma \triangleright P = Q,\ \Gamma \triangleright Q = R}{\Gamma \triangleright P = R}$$

(16) $$\frac{}{\mathbf{F} \triangleright P = Q}$$ where $\mathbf{F}$ denotes the constant false formula.

(17) $$\frac{\Gamma_1 \triangleright P = Q,\ \Gamma_2 \triangleright P = Q,\ \Gamma \models \Gamma_1 \vee \Gamma_2}{\Gamma \triangleright P = Q}$$

(18) $$\frac{}{\Gamma \triangleright \varepsilon(\Phi_1 \vee \Phi_2, \Phi_3).P = \varepsilon(\Phi_1, \Phi_3).P + \varepsilon(\Phi_2, \Phi_3).P}$$

(19) $$\frac{}{\Gamma \triangleright \varepsilon(\Phi_1, \Phi_2 \vee \Phi_3).P = \varepsilon(\Phi_1, \Phi_2).P + \varepsilon(\Phi_1, \Phi_3).P}$$

(20) $$\frac{}{\Gamma \triangleright a(\Phi_1 \vee \Phi_2, \Phi_3).P = a(\Phi_1, \Phi_3).P + a(\Phi_2, \Phi_3).P}$$

(21) $$\frac{}{\Gamma \triangleright a(\Phi_1, \Phi_2 \vee \Phi_3).P = a(\Phi_1, \Phi_2).P + a(\Phi_1, \Phi_3).P}$$

Remark: A special case of Rule (17) is the Rule CONS: $\frac{\Gamma' \triangleright P = Q,\ \Gamma \models \Gamma'}{\Gamma \triangleright P = R}$

We write $\vdash \Gamma \triangleright P = Q$ to mean that $\Gamma \triangleright P = Q$ can be derived from this proof system.

B. Soundness and Completeness of Inference System

In this section, we study the soundness and completeness of inference system.

We firstly give the soundness of inference system.

Proposition 2. $\vdash \Gamma \triangleright P = Q \Rightarrow P \sim_S^\Gamma Q$.

Proof. By induction on the length of inference. The base case when the length is 0 is straightforward. For the induction step we do case analysis on the last rule applied. ■

Now we turn to completeness. To prove the completeness of inference system, we give the following definitions and lemmas.

Definition 5. A standard equation set

$E : \{X_i = \Sigma_{l\in L}\varepsilon(\Phi_{l1}, \Phi_{l2}).X_l + \Sigma_{m\in M}a_m(\Psi_{m1}, \Psi_{m2}).X_m + \Sigma_{n\in N}W_n \mid i \in I\}$

is an equation set with formal process variables in $\{X_i\}$ and free process variables in $\{W_j \mid j \in J\}$. E is closed if $\{W_j \mid j \in J\} = \emptyset$.

Definition 6. A process P provably $\Gamma-$satisfy an equation set E ($\{X_i = Q_i \mid i \in I\}$) if there exist a vector of processes $\{P_i \mid i \in I\}$ and a condition Γ such that $\vdash \Gamma \triangleright P_1 = P$, and $\vdash \Gamma \triangleright P_i = Q_i\{P_j/X_j\}$ for each $i \in I$. We will simply say "provably satisfies E" when $\Gamma = \mathbf{T}$, where $\mathbf{T}$ denotes the constant true formula.

The following lemma states that any process can be represented as a standard equation set.

Lemma 5. For any process P with free process variables W there exists a standard equation set E, with free process variables in W, which is provably satisfied by P. In particular, if P is closed then E is also closed.

$Proof$. See Appendix D. ■

The following lemma shows that two bisimilar processes can be represented as same standard equation set.

Lemma 6. For closed processes P and Q, if $P \sim_S^\Gamma Q$ then there exist a standard, closed equation set E, which is provably $\Gamma-$satisfied by both P and Q.

$Proof$. See Appendix E. ■

The following lemma states that two processes can be proved to be equivalent if they can be represented as same standard equation set.

Lemma 7. If both P and Q provably $\Gamma-$satisfy an equation set E then $\vdash \Gamma \triangleright P = Q$.

$Proof$. See Appendix F. ■

Now we prove the completeness of inference system.

Proposition 3. For closed processes P and Q, $P \sim_S^\Gamma Q \Rightarrow \vdash \Gamma \triangleright P = Q$.

$Proof$. By Lemma 6, there is a standard equation set E such that which are $\Gamma'-$satisfied by both P and Q for some Γ' such that $\Gamma' \Rightarrow \Gamma$. By Lemma 6, $\vdash \Gamma' \triangleright P = Q$. Finally, by Rule CONS, $\vdash \Gamma' \triangleright P = Q$. ■

The soundness and completeness of inference system is given as follows.

Proposition 4. For closed processes P and Q, $P \sim_S^\Gamma Q \Leftrightarrow \vdash \Gamma \triangleright P = Q$.

$Proof$. By Proposition 2 and Proposition 3. ■

Since concrete bisimulation is equivalent to symbolic bisimulation, the inference system is also sound and complete for concrete bisimulation.

Proposition 5. For any $\rho \models \Gamma$, $\langle P, \rho\rangle \sim \langle Q, \rho\rangle \Leftrightarrow \vdash \Gamma \triangleright P = Q$.

$Proof$. By Proposition 1 and Proposition 4. ■

V. CONCLUSIONS

There are many works on hybrid systems such as [2], [3], [4], [7], and [12]. But as far as we know, there are seldom works on sound and complete inference systems for bisimulation of hybrid systems. However, the sound and complete inference systems for some special kind of hybrid system, such as real timed system, have been proposed. In [11], a timed process calculus where processes denotes timed automata was proposed. Then a complete inference system for such a timed process calculus was presented.

The main aim of this paper is to present a sound and complete inference system for bisimulation of hybrid systems. This paper proposed a hybrid process calculus firstly. Then the concrete bisimulation and symbolic bisimulation for this hybrid process calculus were presented and the equivalence between the two bisimulations were proved. We proposed an inference system for symbolic bisimulation. Furthermore, the soundness and completeness of the inference system were also proved.

ACKNOWLEDGMENT

This work was supported by the Aviation Science Fund of China under Grant No. 20128052064 and the National Natural Science Foundation of China under Grant No. 60873025.

REFERENCES

[1] R. Alur and D. L. Dill. A theory of timed automata. Theoretical Computer Science, 126: 1994, pp. 183-235.

[2] J.A.Bergstra and C.A.Middelburg. Process Algebra for Hybrid Systems, Theoretical Computer Science 335, 2005, pp. 215-280.

[3] D.A. van Beek, K.L. Man, M.A. Reniers, J.E. Rooda, and R. Schiffelers. Syntax and Consistent Equation Semantics of Hybrid Chi, Journal of Logic and Algebraic Programming 68, 2006, pp. 129-210.

[4] P.J. Cuijpers and M.A. Reniers. Hybrid Process Algebra, Journal of Logic and Algebraic Programming 62, 2005, pp. 191-245.

[5] Jan Friso Groote and Alban Ponse. The Syntax and Semantics of μCRL, Report, Stichting Mathematisch Centrum, 1990, 35 pages.

[6] Jifeng H. From CSP to hybrid Systems, in A.W.Roscoe(Ed.), A Classical Mind: Essays in honour of C.A.R. Hoare, Prentice hall, Englewood Cliffs, NJ, 1994, pp. 171-189.

[7] Thomas A. Henzinger. The Theory of Hybrid Automata. In the Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science (LICS 96), 1996, pp. 278-292.

[8] M. Hennessy, H. Lin. Symbolic bisimulations. Theoretical Computer Science, 138(2), 1995, pp. 353-389.

[9] Uzma Khadim. A Comparative Study of Process Algebras for Hybrid Systems. Report, Technische Universiteit Eindhoven, 2006. 108 pages.

[10] N. Lynch, R. Segala, and F.W. Vaandrager, Hybrid I/O automata, Information and Computation 185 (1), 2003, pp.105-157.

[11] H. Lin and W. Yi. Axiomatising Timed Automata. In FST&TCS 2000, LNCS 1974, 2000, pp. 277-289.

[12] W. Rounds and H. Song. The ϕ-calculus: a language for distributed con- trol of reconfigurable embedded systems, In the Proceedings of HSCC 2003, LNCS 2623, 2003, pp. 435-449, Springer-Verlag.

Appendix A. Proof of Lemma 1

Lemma 1. There exists ρ such that $\rho \cup \rho' \models \Gamma \Leftrightarrow \rho' \models (\exists x_1 ... \exists x_m.\Gamma)$, where the domain of ρ is $\{x_1, ..., x_m\}$, the domain of ρ' is $\{y_1, ..., y_n\}$, $\{x_1, ..., x_m\} \cap \{y_1, ..., y_n\} = \emptyset$.

$Proof$. $\Rightarrow$: Suppose there exists ρ such that $\rho \cup \rho' \models \Gamma$, where the domain of ρ is $\{x_1, ..., x_m\}$, the domain of ρ' is

$\{y_1, ..., y_n\}$, $\{x_1, ..., x_m\} \cap \{y_1, ..., y_n\} = \emptyset$. It is immediately that $\rho' \models (\exists x_1 ... \exists x_m.\Gamma)$.

$\Leftarrow$: Suppose $\rho' \models (\exists x_1 ... \exists x_m.\Gamma)$, where the domain of ρ' is $\{y_1, ..., y_n\}$, $\{x_1, ..., x_m\} \cap \{y_1, ..., y_n\} = \emptyset$. Then there is ρ such that the domain of ρ is $\{x_1, ..., x_m\}$, $\rho \cup \rho' \models \Gamma$. ■

Appendix B. Proof of Lemma 2

Lemma 2. (1) Given Γ and Γ', if for any $\rho \models \Gamma$, there is ρ', such that $\rho' \models \Gamma'$, $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Phi_2$, and $\langle P, \rho\rangle \overset{\varepsilon(\Phi_1,\Phi_2),T}{\longrightarrow} \langle P', \rho'\rangle$, then $P \overset{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'}{\longrightarrow} P'$, where $\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_1\{t+\delta/t\}$, $\models (\exists \vec{X}.(\Gamma \wedge \Phi_2 \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$;

(2) Given Γ and Γ', if for any $\rho \models \Gamma$, there is ρ', such that $\rho' \models \Gamma'$, $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Psi_2$, and $\langle P, \rho\rangle \overset{a(\Psi_1,\Psi_2)}{\longrightarrow} \langle P', \rho'\rangle$, then $P \overset{\Gamma,a(\Psi_1,\Psi_2),\Gamma'}{\longrightarrow} P'$, where $\models \Gamma \rightarrow \Psi_1$, $\models (\exists \vec{X}.(\Gamma \wedge \Psi_2))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$;

(3) $P \overset{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'}{\longrightarrow} P'$ implies for any $\rho \models \Gamma$, there is ρ', such that $\rho' \models \Gamma'$ and $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Phi_2$, $\langle P, \rho\rangle \overset{\varepsilon(\Phi_1,\Phi_2),T}{\longrightarrow} \langle P', \rho'\rangle$, where $\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_1\{t+\delta/t\}$, $\models (\exists \vec{X}.(\Gamma \wedge \Phi_2 \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$;

(4) $P \overset{\Gamma,a(\Psi_1,\Psi_2),\Gamma'}{\longrightarrow} P'$ implies for any $\rho \models \Gamma$, there is ρ', such that $\rho' \models \Gamma'$ and $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Psi_2$, $\langle P, \rho\rangle \overset{a(\Psi_1,\Psi_2)}{\longrightarrow} \langle P', \rho'\rangle$, where $\models \Gamma \rightarrow \Psi_1$, $\models (\exists \vec{X}.(\Gamma \wedge \Psi_2))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$.

Proof. By induction on the inference length.

(1) Suppose for any $\rho \models \Gamma$, there is ρ', $\rho' \models \Gamma'$ and $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Phi_2$, $\langle P, \rho\rangle \overset{\varepsilon(\Phi_1,\Phi_2),T}{\longrightarrow} \langle P', \rho'\rangle$. We only discuss the case $\langle \varepsilon(\Phi_1, \Phi_2).P, \rho\rangle \overset{\varepsilon(\Phi_1,\Phi_2),T}{\longrightarrow} \langle P, \rho'\rangle$. Other cases are similar or trivial.

Suppose for any $\rho \models \Gamma$, there is ρ', $\rho' \models \Gamma'$ and $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Phi_2$, $\langle \varepsilon(\Phi_1, \Phi_2).P, \rho\rangle \overset{\varepsilon(\Phi_1,\Phi_2),T}{\longrightarrow} \langle P, \rho'\rangle$. We have $\forall \delta \in [0,T].\rho[t \leftarrow \rho(t)+\delta] \models \Phi_1$, $\rho'(t) = \rho(t)+T$, $\rho \cup (\rho'[x \Leftarrow x']) \models \Phi_2$. Therefore $\varepsilon(\Phi_1, \Phi_2).P \overset{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'}{\longrightarrow} P$, where $\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_1\{t+\delta/t\}$, $\models (\exists \vec{X}.(\Gamma \wedge \Phi_2 \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$.

(2) Suppose for any $\rho \models \Gamma$, there is ρ', $\rho' \models \Gamma'$ and $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Psi_2$, $\langle P, \rho\rangle \overset{a(\Psi_1,\Psi_2)}{\longrightarrow} \langle P', \rho'\rangle$. Similar to Case (1).

(3) Suppose $P \overset{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'}{\longrightarrow} P'$. We only discuss the case $\varepsilon(\Phi_1, \Phi_2).P \overset{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'}{\longrightarrow} P$. Other cases are similar or trivial.

Suppose $\varepsilon(\Phi_1, \Phi_2).P \overset{\Gamma,(\varepsilon(\Phi_1,\Phi_2),T),\Gamma'}{\longrightarrow} P$. We have $\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_1\{t+\delta/t\}$, $\models (\exists \vec{X}.(\Gamma \wedge \Phi_2 \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'$. Therefore $\langle \varepsilon(\Phi_1, \Phi_2).P, \rho\rangle \overset{\varepsilon(\Phi_1,\Phi_2),T}{\longrightarrow} \langle P, \rho'\rangle$, where $\forall \delta \in [0,T].\rho[t \leftarrow \rho(t)+\delta] \models \Phi_1$, $\rho'(t) = \rho(t)+T$, $\rho \cup (\rho'[x \Leftarrow x']) \models \Phi_2$.

(4) Suppose $P \overset{\Gamma,a(\Psi_1,\Psi_2),\Gamma'}{\longrightarrow} P'$. Similar to Case (3). ■

Appendix C. Proof of Proposition 1

Proposition 1. For any $\rho \models \Gamma$, $\langle P, \rho\rangle \sim \langle Q, \rho\rangle \Leftrightarrow P \sim_S^\Gamma Q$.

Proof. $\Rightarrow$: Let $R = \{(P, Q) \mid \langle P, \rho\rangle \sim \langle Q, \rho\rangle$ for any $\rho \models \Gamma\}$. It is enough to prove that $R \subseteq \sim_S^\Gamma$.

It holds that $P \sim_S^\Gamma \Sigma_{l\in L}\varepsilon(\Phi_{l1}, \Phi_{l2}).P_l + \Sigma_{m\in M}a_m(\Psi_{m1}, \Psi_{m2}).P_m$ and $Q \sim_S^\Gamma \Sigma_{o\in O}\varepsilon(\Phi_{o1}, \Phi_{o2}).Q_o + \Sigma_{p\in P}a_p(\Psi_{p1}, \Psi_{p2}).Q_p$ by Lemma 3 and Lemma 4.

(1) Since $\langle P, \rho\rangle \sim \langle Q, \rho\rangle$, we have that $\Gamma \models (\vee_{l\in L}\Phi_{l1}) \leftrightarrow (\vee_{o\in O}\Phi_{o1})$, $\Gamma \models (\vee_{l\in L}\Phi_{l2}) \leftrightarrow (\vee_{o\in O}\Phi_{o2})$, $\Gamma \models (\vee_{m\in M}\Psi_{m1}) \leftrightarrow (\vee_{p\in P}\Psi_{p1})$, and $\Gamma \models (\vee_{m\in M}\Psi_{m2}) \leftrightarrow (\vee_{p\in P}\Psi_{p2})$, otherwise P can perform some action that Q can not, and that is a contradiction. Therefore, $\Gamma \models \vee_{l\in L,o\in O}(\Phi_{l1} \wedge \Phi_{o1}) \leftrightarrow \vee_{l\in L}\Phi_{l1} \leftrightarrow \vee_{o\in O}\Phi_{o1}$ and $\{\Phi_{l1} \wedge \Phi_{o1} \mid l \in L, o \in O\}$ is a finite partition of $\vee_{l\in L}\Phi_{l1}$ and $\vee_{o\in O}\Phi_{o1}$. Similarly, there is a finite partition of $(\vee_{l\in L}\Phi_{l2})$ and $(\vee_{o\in O}\Phi_{o2})$, a finite partition of $(\vee_{m\in M}\Psi_{m1})$ and $(\vee_{p\in P}\Psi_{p1})$, and a finite partition of $(\vee_{m\in M}\Psi_{m2})$ and $(\vee_{p\in P}\Psi_{p2})$.

Suppose $\langle P, \rho\rangle \overset{\varepsilon(\Phi_{l1},\Phi_{l2}),T}{\longrightarrow} \langle P', \rho'\rangle$ for any $\rho \models \Gamma$. By Lemma 2, $P \overset{\Gamma,(\varepsilon(\Phi_{l1},\Phi_{l2}),T),\Gamma'_P}{\longrightarrow} P'$, where $\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_{l1}\{t+\delta/t\}$, $\models (\exists \vec{X}.(\Gamma \wedge \Phi_{l2} \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'_P$. Since $\langle P, \rho\rangle \sim \langle Q, \rho\rangle$, by Lemma 2 and Lemma 4, we have that there exists a finite partition $\Sigma = \{\Gamma \wedge \Phi_{l1} \wedge \Phi_{o1} \mid l \in L, o \in O\}$, $\models \Gamma \wedge \Phi_{l1} \leftrightarrow \vee_{o\in O}(\Gamma \wedge \Phi_{l1} \wedge \Phi_{o1})$, for any $\Gamma \wedge \Phi_{l1} \wedge \Phi_{o1}$, there exists a finite partition $\Pi = \{\Gamma \wedge \Phi_{l2} \wedge \Phi_{o2}\}$, $\models \Gamma \wedge \Phi_{l1} \wedge \Phi_{o1} \wedge \Phi_{l2} \leftrightarrow \vee_{o\in O}(\Gamma \wedge \Phi_{l2} \wedge \Phi_{o2})$, for any $\Gamma \wedge \Phi_{l2} \wedge \Phi_{o2}$, there exists Q' such that $Q \overset{\Gamma,(\varepsilon(\Phi_{o1},\Phi_{o2}),T),\Gamma'_Q}{\longrightarrow} Q'$ and $\Gamma \wedge \Phi_{l1} \wedge \Phi_{o1} \models \Gamma \wedge \Phi_{o1}$, $\Gamma \wedge \Phi_{l2} \wedge \Phi_{o2} \models \Gamma \wedge \Phi_{o2}$ and $P' \ R^{(\exists \vec{X}.(\Gamma \wedge \Phi_{l2} \wedge \Phi_{o2} \wedge t' = t+T))\{\vec{X} / \vec{X'}\}} \ Q'$.

(2) In the case of $P \overset{\Gamma,a_m(\Psi_{m1},\Psi_{m2}),\Gamma'_P}{\longrightarrow} P'$, proof is similar to Case (1).

$\Leftarrow$: Let $R = \{(\langle P, \rho\rangle, \langle Q, \rho\rangle) \mid P \sim_S^\Gamma Q$ where $\rho \models \Gamma\}$. It is enough to prove that $R \subseteq \sim$.

(1) Suppose $P \sim_S^\Gamma Q$. It holds that $P \sim_S^\Gamma \Sigma_{l\in L}\varepsilon(\Phi_{l1}, \Phi_{l2}).P_l + \Sigma_{m\in M}a_m(\Psi_{m1}, \Psi_{m2}).P_m$ and $Q \sim_S^\Gamma \Sigma_{o\in O}\varepsilon(\Phi_{o1}, \Phi_{o2}).Q_o + \Sigma_{p\in P}a_p(\Psi_{p1}, \Psi_{p2}).Q_p$ by Lemma 3 and Lemma 4. We have that $\Gamma \models (\vee_{l\in L}\Phi_{l1}) \leftrightarrow (\vee_{o\in O}\Phi_{o1})$, $\Gamma \models (\vee_{l\in L}\Phi_{l2}) \leftrightarrow (\vee_{o\in O}\Phi_{o2})$, $\Gamma \models (\vee_{m\in M}\Psi_{m1}) \leftrightarrow (\vee_{p\in P}\Psi_{p1})$, and $\Gamma \models (\vee_{m\in M}\Psi_{m2}) \leftrightarrow (\vee_{p\in P}\Psi_{p2})$, otherwise P can perform some action that Q can not, and that is a contradiction. Therefore, $\Gamma \models \vee_{l\in L,o\in O}(\Phi_{l1} \wedge \Phi_{o1}) \leftrightarrow \vee_{l\in L}\Phi_{l1} \leftrightarrow \vee_{o\in O}\Phi_{o1}$ and $\{\Phi_{l1} \wedge \Phi_{o1} \mid l \in L, o \in O\}$ is a finite partition of $\vee_{l\in L}\Phi_{l1}$ and $\vee_{o\in O}\Phi_{o1}$. Similarly, there is a finite partition of $(\vee_{l\in L}\Phi_{l2})$ and $(\vee_{o\in O}\Phi_{o2})$, a finite partition of $(\vee_{m\in M}\Psi_{m1})$ and $(\vee_{p\in P}\Psi_{p1})$, and a finite partition of $(\vee_{m\in M}\Psi_{m2})$ and $(\vee_{p\in P}\Psi_{p2})$.

Suppose $P \overset{\Gamma,(\varepsilon(\Phi_{l1},\Phi_{l2}),T),\Gamma'_P}{\longrightarrow} P'$. By Lemma 2, for any $\rho \models \Gamma$, there is ρ', $\rho' \models \Gamma'_P$ and $\rho \cup (\rho'[x \Leftarrow x']) \models \Gamma \wedge \Phi_{l2}$, $\langle P, \rho\rangle \overset{\varepsilon(\Phi_{l1},\Phi_{l2}),T}{\longrightarrow} \langle P', \rho'\rangle$, where $\models \forall \delta \in [0,T].\Gamma\{t+\delta/t\} \rightarrow \Phi_{l1}\{t+\delta/t\}$, $\models (\exists \vec{X}.(\Gamma \wedge \Phi_{l2} \wedge t' = t+T))\{\vec{X} / \vec{X'}\} \rightarrow \Gamma'_P$.

Since $P \sim_S^\Gamma Q$, we have that there exists a finite partition $\Sigma = \{\phi_i \mid i \in I\}$, $\models \Gamma \wedge \Phi_{l1} \leftrightarrow \vee_{i\in I}\phi_i$, for any ϕ_i, there exists a finite partition $\Pi = \{\chi_j \mid j \in J\}$, $\models \phi_i \wedge \Phi_{l2} \leftrightarrow \vee_{j\in J}\chi_j$, for any χ_j, there exists Q' such that $Q \stackrel{\Gamma,(\varepsilon(\Phi_{o1},\Phi_{o2}),T),\Gamma'_Q}{\longrightarrow} Q'$ and $\phi_i \models \Gamma \wedge \Phi_{o1}$, $\chi_j \models \Gamma \wedge \Phi_{o2}$ and $P'\ R^{(\exists \vec{X}.\chi_j \wedge t' = t+T)\{\vec{X}/\vec{X'}\}}\ Q'$. Hence $\rho \models \phi_i \models \Gamma \wedge \Phi_{o1}$ and $\rho' \models (\exists\ \vec{X}\ .\chi_j \wedge t' = t+T)\{\vec{X}\ /\ \vec{X'}\} \models (\exists\ \vec{X}\ .\Gamma \wedge \Phi_{o2} \wedge t' = t+T)\{\vec{X}\ /\ \vec{X'}\}$. Therefore by Lemma 2 we have that there exists Q' such that $\langle Q, \rho\rangle \stackrel{\varepsilon(\Phi_{o1},\Phi_{o2}),T}{\longrightarrow} \langle Q', \rho'\rangle$ and $\langle P', \rho'\rangle\ R\ \langle Q', \rho'\rangle$.

(2) In the case of $\langle P, \rho\rangle \stackrel{a_m(\Psi_{m1},\Psi_{m2})}{\longrightarrow} \langle P', \rho'\rangle$, proof is similar to Case (1). ■

Appendix D. Proof of Lemma 5

Lemma 5. For any process P with free process variables W there exists a standard equation set E, with free process variables in W, which is provably satisfied by P. In particular, if P is closed then E is also closed.

Proof. By induction on the structure of P. The only non-trivial case is recursion when $P \equiv fixX.P'$. By induction, there is a standard equation set $E' : \{X_i = U_i \mid i \in I\}$ with free process variables in $FV(P) \cup \{X\}$ and P'_i such that $\vdash P' = P'_1$ and $\vdash P'_i = U_i\{P'_j/X_j \mid j \in I\}$.

We may assume that X is different from any X_i. Let $V_i = U_i\{U_1/X\}$ for each $i \in I$. Note that since X is under an action prefixing in P', it does not occur free in U_1. Hence $V_1 = U_1$. Consider the equation set $E : \{X_i = V_i \mid i \in I\}$. Set $P_i = P'_i\{P/X\}$. Then $\vdash P = fixX.P' = fixX.P'_1 = P'_1\{fixX.P'_1/X\} = P'_1\{P/X\} = P_1$ and $\vdash P = P'_1\{P/X\} = U_1\{P'_i/X_i \mid i \in I\}\{P/X\} = U_1\{P'_i\{P/X\}/X_i \mid i \in I\} = U_1\{P_i/X_i \mid i \in I\}$. Now $\vdash P_i = P'_i\{P/X\} = U_i\{P'_j/X_j \mid j \in I\}\{P/X\} = U_i\{P, P'_j\{P/X\}/X, X_j \mid j \in I\} = U_i\{P, P_j/X, X_j \mid j \in I\} = U_i\{U_1\{P_j/X_j \mid j \in I\}, P'_j\{P/X\}/X, X_j \mid j \in I\} = U_i\{U_1/X\}\{P_j/X_j \mid j \in I\} = V_i\{P_j/X_j \mid j \in I\}$. This shows that P satisfies E. ■

Appendix E. Proof of Lemma 6

Lemma 6. For closed processes P and Q, if $P \sim_S^\Gamma Q$ then there exist a standard, closed equation set E, which is provably $\Gamma-$satisfied by both P and Q.

Proof. Let E_1 and E_2 be the standard equation sets for P and Q, respectively: $E_1 : \{X_i = \Sigma_{l\in L}\varepsilon(\Phi_{l1}, \Phi_{l2}).X_l + \Sigma_{m\in M}a_m(\Psi_{m1}, \Psi_{m2}).X_m + \Sigma_{n\in N}W_n \mid i \in I\}$, $E_2 : \{Y_j = \Sigma_{o\in O}\varepsilon(\Phi_{o1}, \Phi_{o2}).X_o + \Sigma_{p\in P}b_p(\Psi_{p1}, \Psi_{p2}).X_p + \Sigma_{q\in Q}W_q \mid j \in J\}$. So there are P_i, Q_j such that $\vdash P_1 = P$, $\vdash Q_1 = Q$, and $\vdash P_i = \Sigma_{l\in L}\varepsilon(\Phi_{l1}, \Phi_{l2}).P_l + \Sigma_{m\in M}a_m(\Psi_{m1}, \Psi_{m2}).P_m$, $\vdash Q_j = \Sigma_{o\in O}\varepsilon(\Phi_{o1}, \Phi_{o2}).Q_o + \Sigma_{p\in P}b_p(\Psi_{p1}, \Psi_{p2}).Q_p$. Without loss of generality, we may assume $a_m = b_p = a$ for all m, p.

Define $E : \{Z_{ij} = \Sigma_{l\in L,o\in O}\varepsilon(\Phi_{l1} \wedge \Phi_{o1}, \Phi_{l2} \wedge \Phi_{o2}).Z_{lo} + \Sigma_{m\in M,p\in P}a(\Psi_{m1} \wedge \Psi_{p1}, \Psi_{m2} \wedge \Psi_{p2}).Z_{mp} + \Sigma_{n\in N,q\in Q}Z_{nq} \mid i \in I, j \in J\}$.

We claim that E is provably $\Gamma-$satisfied by P when each Z_{ij} is instantiated with P_i.

We need to show, for each i, $\vdash \Gamma \triangleright P_i = \Sigma_{l\in L,o\in O}\varepsilon(\Phi_{l1} \wedge \Phi_{o1}, \Phi_{l2} \wedge \Phi_{o2}).P_l + \Sigma_{m\in M,p\in P}a(\Psi_{m1} \wedge \Psi_{p1}, \Psi_{m2} \wedge \Psi_{p2}).P_m$.

Since $P \sim_S^\Gamma Q$, we have for any l, $\Phi_{l1} \wedge \neg(\vee_{o\in O}\Phi_{o1}) = \mathbf{F}$, $\Phi_{l2} \wedge \neg(\vee_{o\in O}\Phi_{o2}) = \mathbf{F}$, and for any m, $\Psi_{m1} \wedge \neg(\vee_{p\in P}\Psi_{p1}) = \mathbf{F}$, $\Psi_{m2} \wedge \neg(\vee_{p\in P}\Psi_{p2}) = \mathbf{F}$.

Therefore, $\vdash\ \Gamma \triangleright \Sigma_{l\in L,o\in O}\varepsilon(\Phi_{l1} \wedge \Phi_{o1}, \Phi_{l2} \wedge \Phi_{o2}).P_l + \Sigma_{m\in M,p\in P}a(\Psi_{m1} \wedge \Psi_{p1}, \Psi_{m2} \wedge \Psi_{p2}).P_m$

$= \Sigma_{l\in L,o\in O}\varepsilon(\Phi_{l1} \wedge \Phi_{o1}, \Phi_{l2} \wedge \Phi_{o2}).P_l + 0 + 0 + \Sigma_{m\in M,p\in P}a(\Psi_{m1} \wedge \Psi_{p1}, \Psi_{m2} \wedge \Psi_{p2}).P_m + 0 + 0$

$= \Sigma_{l\in L,o\in O}\varepsilon(\Phi_{l1} \wedge \Phi_{o1}, \Phi_{l2} \wedge \Phi_{o2}).P_l + \Sigma_{l\in L,o\in O}\varepsilon(\Phi_{l1} \wedge \neg(\vee_{o\in O}\Phi_{o1}), \Phi_{l2} \wedge \Phi_{o2}).P_l + \Sigma_{l\in L,o\in O}\varepsilon(\Phi_{l1} \wedge \Phi_{o1}, \Phi_{l2} \wedge \neg(\vee_{o\in O}\Phi_{o2})).P_l + \Sigma_{m\in M,p\in P}a(\Psi_{m1} \wedge \Psi_{p1}, \Psi_{m2} \wedge \Psi_{p2}).P_m + \Sigma_{m\in M,p\in P}a(\Psi_{m1} \wedge \neg(\vee_{p\in P}\Psi_{p1}), \Psi_{m2} \wedge \Psi_{p2}).P_m + \Sigma_{m\in M,p\in P}a(\Psi_{m1} \wedge \Psi_{p1}, \Psi_{m2} \wedge \neg(\vee_{p\in P}\Psi_{p2})).P_m$

$= \Sigma_{l\in L}\varepsilon(\Phi_{l1}, \Phi_{l2}).P_l + \Sigma_{m\in M}a(\Psi_{m1}, \Psi_{m2}).P_m = P_i$

Symmetrically we can show that E is provably $\Gamma-$satisfied by Q when each Z_{ij} is instantiated with Q_j. ■

Appendix F. Proof of Lemma 7

Lemma 7. If both P and Q provably $\Gamma-$satisfy an equation set E then $\vdash \Gamma \triangleright P = Q$.

Proof. By induction on the size of E. For the base case when E contains only one equation $X_1 = V_1$, we have $\vdash \Gamma \triangleright P = V_1\{P/X_1\}$. Therefore $\vdash \Gamma \triangleright P = fixX_1.V_1$. Similarly, $\vdash \Gamma \triangleright Q = fixX_1.V_1$. Hence $\vdash \Gamma \triangleright P = Q$.

Assume the result for m and let E contain $m+1$ equations: $X_i = V_i$, $1 \le i \le m+1$. Since P provably $\Gamma-$satisfies E, there are P_i, $1 \le i \le m+1$, such that $\vdash \Gamma \triangleright P_1 = P$, and $\vdash \Gamma \triangleright P_i = V_i\{P_j/X_j\}$ for each $1 \le i, j \le m+1$. In particular, $\vdash \Gamma \triangleright P_{m+1} = V_{m+1}\{P_i/X_i \mid 1 \le i \le m+1\} = (V_{m+1}\{P_i/X_i \mid 1 \le j \le m\})\{P_{m+1}/X_{m+1}\}$. By Rule (11), $\vdash \Gamma \triangleright P_{m+1} = fixX_{m+1}.V_{m+1}\{P_i/X_i \mid 1 \le i \le m\}$. Writing W_{m+1} for $fixX_{m+1}.V_{m+1}$, we have $\vdash\ \Gamma \triangleright P_{m+1} = W_{m+1}\{P_i/X_i \mid 1 \le i \le m\}$. Therefore, $\vdash\ \Gamma \triangleright P_i = V_i\{P_j/X_j \mid 1 \le j \le m+1\} = V_i\{P_j/X_j \mid 1 \le j \le m\}\{P_{m+1}/X_{m+1}\} = V_i\{P_j/X_j \mid 1 \le j \le m\}\{W_{m+1}\{P_i/X_i \mid 1 \le i \le m\}/X_{m+1}\} = V_i\{W_{m+1}/X_{m+1}\}\{P_j/X_j \mid 1 \le j \le m\}$. This shows P provably $\Gamma-$satisfies the equation set $E' : X_i = V_i\{W_{m+1}/X_{m+1}\}$ for each $1 \le i \le m$. Symmetrically we can show that Q provably $\Gamma-$satisfies the equation set E'. By induction we conclude $\vdash \Gamma \triangleright P = Q$. ■